

23 August 1977

MEMORANDUM FOR: Office of General Counsel

ATTENTION :

FROM :

SUBJECT : Comments on Preliminary Draft of Revised
Executive Order on Classification

REFERENCE : Multiple addressee memorandum dtd 9 Aug
from Office of General Counsel re
PRM/NSC-29: Revision of Executive
Order 11652

1. Overall we find the proposed draft acceptable. Some sections will give us a little difficulty in implementation and these minor points are explained below.

Section 1. Definitions (d)

"Intelligence source" means a person or organization which provides foreign intelligence to the United States only on the condition that its identity remains undisclosed.

The implication in the definition is that if the person (organization) does not specifically request its identity remain undisclosed, it is not classifiable and may, in fact, be disclosed. The Agency protects its sources whether or not they request we do so. Often the simple fact of cooperation with CIA would endanger the source and the relationship. We suggest the deletion of "only" in the definition to eliminate the implication of disclosability.

Section 2.(a) Classification Requirements (2)

The disclosure of such (i.e., classified) information could reasonably be expected to cause at least significant damage to the national security.

The use of the qualifier "significant" seems to exclude protection for Agency officers serving under cover and similar kinds of sources and methods information which, if disclosed could cause damage to intelligence operations but hardly "significant damage" to the national security itself. We would be more comfortable with removal of the phrase "at least significant" in the above statement.

Section 2.(b) Classification Criteria (8)

The info was provided in confidence by a foreign government or international organization; or the info would reveal the identity of any other foreign source who has requested that his identity remain confidential.

Here again, the justification for classification implies that if the source requests protection we will do so, but if he does not, we may not classify his identity. Whether or not the source requests confidentiality, we must be able to provide it.

Section 2.(c) Prohibitions (5)

If clearly identified classified information is officially placed in the public domain by an official authorized . . . to declassify such info, that particular information shall no longer be classified.

It should be made perfectly clear that this paragraph refers to information that is officially placed in the public domain and not simply information leaked from an official source.

Section 2.(d) Classification Authority

It is unclear whether the DDCI may authorize Top Secret classification authority. We suggest the wording of Executive Order 11652 be reinserted into the new Order so that the DCI or his principal deputy may delegate Top Secret National Security Classification Authority.

Section 2.(f) Limitation on Authority to Provide for the Duration of Classification

The six year limitation on duration of classification applied by Secret and Confidential

classifiers causes us some concern. Only a small fraction of Agency classified material could be handled in this manner - perhaps a few finished intelligence reports in which the sensitivity expires with age.

We seem to face two reasonable alternatives in complying with this provision. On the one hand we could increase our number of Top Secret classifiers or we could develop classification guidelines for agency-wide promulgation. Currently, the Agency has over 1900 officers with National Security Classification Authority: 26.8 percent at the Top Secret level; 72.1 percent at the Secret level, and 1.1 percent at the Confidential level. If we are to be able to protect our information beyond six years, these percentages will have to shift toward the Top Secret side.

The other alternative would be to develop classification guidelines for approval by a Top Secret classifier. Other agencies have successful classification guides to aid officers in their classification decisions. A good starting point might be the aspects of sources and methods or the declassification guidelines developed by Records Review Branch/DDA.

Section 4. Declassification (2) Guidelines

The Order should state clearly that the only material to be reviewed for declassification is that which is approved by the Archivist for permanent retention.

2. If any of the above points are unclear or need amplification, please contact the undersigned.

[Redacted Signature]

STAT

Distribution:

Original - Addressee

- 1 - RAB [Redacted]
- ~~1~~ - DDA Subject
- 1 - Chrono

STAT

STAT

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300050003-9

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300050003-9

21 Sep 77

Suggested changes to the final (9/13/77) draft of the Executive Order on "National Security Information and Material"

1. Page 2, Table of Contents. Add under the caption for Section 6 a new sub-caption reading "(e) Controls on Reproduction and Distribution," REASON: Consistency with the text of the draft Order.

2. Page 3, Subsection 1(e). Change to read: "'Intelligence method' means...activities of the United States, or which ~~would~~ could, if disclosed, reasonably be expected to lead to...." REASON: Consistency with usage in the first part of the definition and in the definition for an intelligence source; and to provide for the application of judgment to the possible consequences of disclosure.

3. Page 5, Subsection 2(a)(2). Change the second sentence to read: "In the case of information provided in confidence by a foreign government or international organization, and of information specifically bearing on intelligence sources or intelligence methods, it is reasonable to expect that the breach of that confidence, or the disclosure in whole or in part of those sources or methods, could cause at least significant damage to the national security." REASON: (1) The language in the present draft reflects decisions that information provided in confidence by a foreign government, etc., should be treated as classified information, not just classifiable dependent upon a separate finding that its disclosure would cause a requisite degree of damage to the national security. Intelligence sources and intelligence methods are at least as sensitive as foreign governmental confidences. Some intelligence sources are foreign governments. The draft Order defines such sources and methods as being inherently sensitive. As such, information satisfying those definitions should not have to undergo a separate test, subject to litigation under the Freedom of Information Act, of damage to the national security if disclosed. The Order should therefore assert that both classes of information are classified. (2) The qualifier "at least" before "significant damage" is needed to allow whatever classification designation is appropriate to be applied to the information involved. As written, the classification would be limited to Confidential (v. Section 1(f)(3)).

4. Page 5, Subsection 2(b)(3). Change lines 3-5 to read: "Provide a foreign nation with information upon which it could use to develop effective countermeasures to such plans or posture;" REASON: (1) Grammatical; (2) The qualifier "effective" adds a judgmental consideration essentially irrelevant to the application of this classification criterion.

5. Page 8, Subsection 2(c)(7). Change to read: "Where there is doubt whether information should be classified Secret or Top Secret, it shall not be classified Top Secret. Where there is doubt whether information ~~classified~~ should be classified Confidential or Secret, it shall not be classified Secret ~~Confidential~~." REASON: Consistency with the prohibitory language in the other parts of Subsection 2(c).

6. Page 8, Subsection 2(d)(1). Change to read: "The authority to originally classify information 'Top Secret' may be exercised only by such officials as the President by publication in the Federal Register may designate in writing, ~~and, subject to the restriction in paragraph (4)~~ by the heads of the following agencies, and, subject to the restrictions in Subsection (4), by such persons as they may designate in writing:" REASON: (1) To make clear that persons designated in writing by those officials named by the President or by agency heads also have proper authority to classify information. (2) To show that the restriction in Subsection (4) applies to the designation of classifying authorities, not to classifying actions by heads of agencies.

7. Page 9, Subsection 2(d)(2). Change to read: "The authority to originally classify information 'Secret' may be exercised, ~~subject to the restrictions in paragraph (4)~~ only by officials who have 'Top Secret' classification authority, and by the heads of the following agencies, and, subject to the restrictions in Subsection (4), by such persons as they may designate in writing:" REASON: Same as for change 6 above.

8. Page 9, Subsection 2(d)(3). Change to read: "The authority to originally classify information 'Confidential' may be exercised, ~~subject to the restrictions in paragraph (4)~~, only by officials who have 'Top Secret' or 'Secret' classification authority, and by the heads of the following

agencies, and, subject to the restrictions in Subsection (4), by such persons as they may designate in writing:" REASON: Same as for change 6 above.

9. Page 10, Subsection 2(d)(4). Change the word "paragraphs" in line 2 to read "subsections". REASON: Consistency of usage in the Order.

10. Page 10, Subsection 2(d)(4). Delete the third sentence. REASON: The restriction expressed in the sentence on redelegation of "Secret" and "Confidential" classifying authority would place an unreasonable administrative burden on large organizations, especially those with a number of field components having valid reasons for original classification authority. PRM-29 deliberations surfaced no instances of abuse of delegation or redelegation of classification authority. An unsupported assumption that such redelegation might be abused in the future should not justify prohibitory language in the Order. The possibility of such abuse should instead be addressed through inspections and monitoring by the Oversight Office established by the Order.

11. Page 11, Subsection 2(f)(1). Replace with the following: "All original classification authorities shall, at the time of original classification determinations, set a specific date or event for automatic declassification of the information which shall be as early as the national security interest will permit but shall not exceed six years from the date of origin of the information that is classified; except" REASON: To state clearly the obligations of original classification authorities regarding the duration of classifications, and to express these in a manner which clearly shows that the following subsection provides for modification. As written in the draft Order, this subsection does not clearly provide for the extension of classifications beyond six years because the exception clause applies only to the first sentence, which speaks only to the setting of a "specific date or event for automatic declassification".

12. Pages 11-12, Subsection 2(f)(2). Revise to read: "In those cases where there is a need, directly related to the national security, to continue classification beyond six years, only Top Secret classification authorities

or the heads of agencies specifically designated in Section 2(d) of this Order may set a later date or event for automatic declassification. ~~Alternatively, these authorities may, where declassification guidelines issued by heads of agencies prescribe a need for review of specified information upon its 20th anniversary, set a date for review of such information consistent with such guidelines. In either case, These dates~~ or events shall be as early as the national security interest will permit but ~~in no case shall~~ not exceed 20 twenty years from date of origin of the information involved. ~~Additionally, for foreign-originated information, as defined in Section 4(f), these officials may set dates or events for declassification or review which shall not exceed thirty years. When those~~ authorities determine that declassification at or before twenty years from date of origin would be demonstrably harmful to the national security, they may instead specify a declassification review at or before the twentieth anniversary of the information when it falls within the ambit of declassification guides issued by heads of agencies under Section 4(a) hereof. Officials who authorize the extension of classification beyond six years must record on the originator's file copy the reasons for such extension and their identity. The reasons must be specific and must explain why the classification will continue to meet the requirements set forth in Subsection 2(a) above. And except REASON: (1) To place immediately after the language permitting extended classification the language which states the limits of such extensions. (2) To delete from this section for later separate expression in the interests of clarity and completeness the language necessary to reflect the decision that foreign originated classified information may retain its classification for thirty years. (3) To state clearly the sequence of determinations and conditions that need to be met for classifying officials to specify review for declassification vice declassification itself. Further, to include the Attorney General's test of "demonstrable harm" as an initial judgment determination in such cases. The language in the present draft on this matter would invite unthinking specification of a review vice declassification date

whenever the information fell within the ambit of declassification guides which may well be relatively general in nature. (4) To link together the existing two subsections and a new subsection (3) on foreign originated information.

13. Page 12, add a new Subsection 2(f)(3) reading: "(3) In the case of classified information furnished to the United States by a foreign government, international organization, or an official or representative thereof, or produced by the United States jointly with a foreign government or international organization, with the understanding that such information will be kept in confidence, Top Secret classification authorities or the heads of agencies specifically designated in Section 2(d) of this Order may continue the classification of such information for thirty years from date of origin unless the foreign government or international organization involved specifies or agrees to earlier declassification. Officials who authorize the extension of classification of foreign originated information must record on the originator's file copy of the information their identity, the specific foreign source involved, and reference to this section of this Order as the reason for extended classification." REASON: (1) To define foreign originated classified information where the term is first used (moving the definition from Section 4(f) of the present draft). (2) In the interests of clarity, to state, in a subsection separate from the one bearing on the extended classification of U.S. originated classified information, the different rules applicable to foreign originated information (i.e., thirty year maximum duration; recognition that foreign governments may agree to lesser period; lack of need to specify alternative of declassification review, as Section 4(f) of the Order exempts foreign information from automatic declassification).

14. Pages 15 and 16. Change the second lines of Subsections 4(b) and (c) to make the reference read "...Subsection (f) below...." REASON: To avoid confusion as to which Subsection (f) is meant.

15. Page 17, Subsection 4(d). Revise the second sentence to read: "Heads of agencies shall order the review for possible disposal of all

security classified records 20 twenty years old or older which are held in storage areas by the agency or in Federal Records Centers ~~for possible disposal.~~" REASON: To remove an ambiguity.

16. Page 17, Subsection 4(d). Replace the last two sentences (all after the words "in these cases") with the following: "When the head of an agency authorizes continued classification, a specific declassification date for the information shall be stated. When the future sensitivity of the information cannot reasonably be predicted during the twenty year review, a date not more than ten years later may be set for a second review in accordance with the procedures applicable for twenty-year-old information. A specific declassification date must be set after the second review. The head of an agency or the Director of Central Intelligence may, for good cause, seek from the Director of the Security Information Oversight Office a waiver of the ten year limit for second reviews." REASON: (1) To clarify an ambiguous antecedent in the present language, (2) To state the conditions which would justify and accompany a second review, and to avoid confusion, to express such separately from the requirement stated for the twenty year review. (3) To state from whom waivers of the ten-year time limit may be sought.

17. Page 17, Subsection 4(e)(1). Revise the first sentence to read: "All information classified under this or prior Orders, except as noted in Subsection (4) below, shall be subject to...." REASON: To make clear at the outset of this Subsection that there is an exception to its application.

18. Page 18, Subsection 4(f). Replace the first sentence with the following: "Foreign originated classified information, as defined in Subsection 2(f)(3) above, is exempt from the declassification provisions of Section 4 of this Order." REASON: To delete the definitional language which would be moved to Subsection 2(f) of the Order by change No. 13 above.

19. Page 20, Subsection 4(g)(5). Revise the first sentence to read: "In the case of classified information not transferred in accordance with ~~paragraph-(4)-of-this~~ Subsection (4) above,...." REASON: Consistency of usage in the Order.

20. Page 23, Subsection 6(b). Revise the second sentence to read: "The Security Information Oversight Office,..." REASON: Accuracy.

21. Page 26, Subsection 6(e)(1)(v). Revise to read: "Records are maintained by the reproducing office to show the number and distribution of reproduced copies of ~~Secret~~ and Top Secret documents and those documents marked...." REASON: The imposition of a requirement to keep records on copies of Secret documents would create a staggering administrative burden for the Intelligence Community, which needs to reproduce and disseminate quantities of documentation at that classification level to satisfy the minimum needs of consumers and producers. Since there has been no showing that the absence of such a record keeping requirement has contributed to classification abuses, there is no justification for imposing this burden.

22. Page 29, Subsection 7(b)(3). Revise to read: "Designate a subordinate ~~senior-member-of-the-agency-staff~~ who shall conduct an active agency oversight program...." REASON: Conciseness and consistency with the usage of Subsection (4) following.

23. Page 32, Section 10. Revise to read: "Executive Order No. 11652 ...are revoked upon the effective date of this Order." REASON: To make clear that the revocation of the existing Order takes effect when the new Order does, and not when the new Order is signed.

16 Sep 77

September 13, 1977

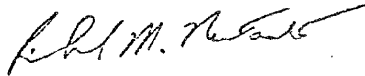
Dear Senator Abourezk:

I am enclosing a copy of a draft Executive Order to replace Order #11652, which establishes the security classification system. In behalf of the President, I would like to request any comments and suggestions you may have. Comments on both policy and specific language would be welcome.

We need your reactions by October 14, 1977, so they can be conveyed to the President before he decides on the final Order. Please send your comments to Ron Kienlen, General Counsel's Office, Office of Management and Budget, Room 465, Old Executive Office Building, Washington, D.C. 20500.

Feel free to share this draft with others who might want to comment. Thanks in advance for your help.

Sincerely,



Richard M. Neustadt
Deputy Special Assistant

The Honorable James Abourezk
Attention of Irene Margolis
United States Senate
Washington, DC 20510

Enclosure

EXECUTIVE ORDER

NATIONAL SECURITY INFORMATION AND MATERIAL

By virtue of the authority vested in me by the Constitution and statutes of the United States of America, and as President of the United States of America, in order to balance the public interest in access to official information with the legitimate need to protect information which should be kept secret in the interest of national security, it is hereby ordered as follows:

TABLE OF CONTENTS

Section	Description
1.	Definitions.....
2.	Original Classification.....
	(a) Classification Requirements.....
	(b) Classification Criteria.....
	(c) Prohibitions.....
	(d) Classification Authority.....
	(e) Exceptional Cases.....
	(f) Limitations on Authority.....
	(g) Identification and Markings.....
3.	Derivative Application of Markings...
4.	Declassification.....
	(a) Guidelines.....
	(b) New Material.....
	(c) Old Material.....

- (d) Systematic Review.....
- (e) Mandatory Review.....
- (f) Foreign Originated ^{Information} ~~Material~~.....
- (g) Declassification Authority.....
- 5. Downgrading.....
- 6. Safeguarding.....
 - (a) Policy Directives.....
 - (b) Secrecy Agreements.....
 - (c) Special Access.....
 - (d) Historical Researchers and Former Officials.....
 - (e) *Controls on Reproduction and Distribution*
- 7. Implementation and Review.....
 - (a) Oversight Office.....
 - (b) ^{Agencies} ~~Departmental~~.....
- 8. Administrative Sanctions.....
- 9. Atomic Energy Material.....
- 10. Revocation of Prior Orders.....
- 11. Effective Date.....

Section 1. Definitions.

(a) "Official information or material" means that information or material which is owned by, produced for or by, or under the control of the United States Government.

(b) "National security" means the foreign policy or national defense interests of the United States. ✓

(c) "Agency" means any independent entity, including the Military Departments, within the Executive Branch.

(d) "Intelligence source" means a person, organization, or technical means which provides foreign intelligence or foreign counterintelligence and which, if its identity or capability is disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in providing foreign intelligence or foreign counterintelligence to the United States. An "intelligence source" also means a person or organization which provides foreign intelligence or foreign counterintelligence to the United States only on the condition that its identity remains undisclosed.

(e) "Intelligence method" means the method which is used to provide support to an intelligence source or operation, and which, if disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in supporting the foreign intelligence or foreign counterintelligence activities of the United States, or which would, if disclosed, reasonably lead to the disclosure of an intelligence source or operation.

(f) "Classified information" is official information which has been determined by proper authority to require a degree of protection against unauthorized disclosure

in the interest of national security and has been designated, dependent upon its significance to the national security, with one of the three following authorized classification designations:

(1) "Top Secret" is the designation which shall be applied to official information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

(2) "Secret" is the designation which shall be applied to official information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

(3) "Confidential" is the designation which shall be applied to official information or material the unauthorized disclosure of which could reasonably be expected to cause significant damage to the national security.

Sec. 2. Original Classification.

(a) Classification Requirements. Official information or material, hereinafter referred to as information, shall not be classified unless an original classification authority determines:

(1) That the information meets one or more of the criteria set forth in subsection (b) below; and

(2) The disclosure of such information could reasonably be expected to cause at least significant damage to the national security. In the case of information provided

in confidence by a foreign government or international organization, ^{SOM} it is reasonable to expect that the breach of that confidence could cause ^{AT LEAST} significant damage to the national security.

(b) Classification Criteria. The following, which apply equally to all three authorized classification designations, describe information which is classifiable if its disclosure could reasonably be expected to:

(1) Make the United States or its allies vulnerable to attack by a foreign power, or weaken the ability of the United States or its allies to conduct armed operations or defend themselves, or diminish the effectiveness of the United States' armed forces; or

(2) Lead to hostile political, economic, or military action against the United States or its allies by a foreign power; or

(3) Disclose, or provide a foreign nation with an insight into, the defense plans or posture of the United States or its allies; provide a foreign nation with information upon which to develop effective countermeasures to such plans or posture; ^{OR} weaken or nullify the effectiveness of a United States military, foreign intelligence, or foreign counterintelligence, plan, operation, project, or activity; or

(4) Aid a foreign nation to develop, improve, or refine its military potential; or

(5) Reveal, jeopardize, or compromise an intelligence source or method, an analytical technique for the interpretation of intelligence data, or a cryptographic device or system; or

(6) Disclose to other nations or foreign groups that the United States has, or is capable of obtaining, certain information or material concerning those nations or groups without their knowledge or consent; or

(7) Deprive the United States of a scientific, engineering, technical, economic, or intelligence advantage directly related to national security; or

(8) Create or increase international tensions; or otherwise significantly impair our foreign relations; or

(9) Disclose or weaken the position of the United States or its allies in the discussion, avoidance, or peaceful resolution of existing or potential international differences; or

(10) Disclose plans prepared by, or under discussion by, officials of the United States to meet contingencies or situations arising in the course of our foreign relations or national defense; or

(11) Cause political or economic instability or civil disorder in a foreign country; or

(12) Disclose the identity of a confidential source of a United States diplomatic or consular post; or

(13) Disclose information or material provided to the United States in confidence by a foreign government or international organization.

c. Prohibitions. Classification of information is subject to the following prohibitions:

(1) Where there is doubt as to whether certain information requires any security protection, the classifying official will strike the balance in favor of public access to official information and the information shall not be classified.

(2) No information may be classified in order to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization, or agency, to restrain competition or independent initiative, or to prevent or delay for any other reason the release of information which does not require, in the interest of national security, the protection authorized by this Order.

(3) Basic scientific research information may not be classified, except for Restricted Data within the meaning of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2014(y)), and except for such information that is directly related to the national security.

(4) Information or material which is not official information or material may not be classified; thus, information resulting from independent or nongovernmental research and development shall not be classified unless it incorporates or reveals classified information to which the researcher or developer was given prior access or unless the Government first acquires a proprietary interest therein.

(5) References to classified documents may not be a basis for classification unless the reference, standing alone, would disclose classified information.

(6) Classification shall not be used solely for the purpose of limiting dissemination of information which is not classifiable under the provisions of this Order.

(7) Where there is doubt whether information should be classified Secret or Top Secret, it shall be classified Secret. Where there is doubt whether information classified should be classified Confidential or Secret, it shall be classified Confidential.

d. Classification Authority.

(1) The authority to originally classify information "Top Secret" may be exercised only by such officials as the President by publication in the Federal Register may designate in writing and, subject to the restriction in paragraph (4) by the heads of the following agencies:

- (i) Department of State
- (ii) Department of the Treasury
- (iii) Department of Defense
- (iv) Department of the Army

- (v) Department of the Navy
- (vi) Department of the Air Force
- (vii) Department of Justice
- (viii) Department of Energy
- (ix) U.S. Arms Control and Disarmament Agency
- (x) Central Intelligence Agency
- (xi) National Aeronautics and Space Administration
- (xii) General Services Administration

(2) The authority to originally classify information "Secret" may be exercised, subject to the restrictions in paragraph (4) only by officials who have Top Secret classification authority and by the heads of the following agencies:

- (i) Department of Commerce
- (ii) Department of Transportation
- (iii) Agency for International Development
- (iv) Office of the Special Representative for Trade Negotiations
- (v) United States Information Agency
- (vi) Nuclear Regulatory Commission

(3) The authority to originally classify information "Confidential" may be exercised, subject to the restrictions in paragraph (4), only by officials who have "Top Secret" or "Secret" classification authority and the heads of the following agencies:

- (i) Department of Labor
- (ii) Export-Import Bank of the United States
- (iii) Overseas Private Investment Corporation

(4) The heads of agencies specifically named in paragraphs (1), (2) and (3) may delegate their authority to originally classify information. Such delegation may provide for redelegation, except for Top Secret original classification authority. Officials to whom such authority is redelegated may not further redelegate it. All delegations shall be in writing, and shall be granted only to officials by name or title of position held. The number of officials to whom original classification authority is delegated shall be restricted to those officials whose duties and responsibilities necessitate the origination of classified information on a regular and recurring basis.

(5) The head of any agency not specifically granted original classification authority herein may not originally classify information under this Order, unless specifically authorized in writing by the President. Requests for such authority shall be directed to the Security Information Oversight Office, established herein, and shall identify the positions requiring the authority, the classification level required and justification for the granting of such authority.

in FR
active
TS?
(p. 11)

(e) Exceptional Cases. In an exceptional case when a person or agency not authorized to originally classify originates information which is believed to require classification, such person or agency shall protect that information in the manner prescribed by this Order and implementing directives. The information shall be promptly transmitted under appropriate safeguards to the agency having primary interest in the subject matter, or where such agency cannot be identified, to the Director of the Security Information Oversight Office, with a request that a determination be made as to classification.

(f) Limitation on Authority to Provide for the Duration of Classification.

(1) All original classification authorities, except as permitted in paragraph (2) shall, at the time of the original classification determination, set a specific date or event for automatic declassification of the information. The date or event shall be as early as the national security interest will permit; but, in no case shall the date or event exceed six years from the date of origin of the information that is classified. EXCEPT:

(2) In those cases where there is a need, directly related to the national security, to continue classification beyond six years, only Top Secret classification authorities or the heads of agencies specifically designated in Sec. 2(d) of this Order may set a later date or event for automatic

(d) declassification. Alternatively, these authorities may,

where declassification guidelines issued by heads of agencies prescribe a need for review of specified information upon its 20th anniversary, set a date for review (b) of such information consistent with such guidelines.

In either case, these dates or events shall be as early as the national security interest will permit but in no case shall exceed 20 years from date of origin of the

information involved. Additionally, for foreign originated information, as defined in Section 4(f), those officials may set dates or events for declassification or review which shall not exceed thirty years. (l)

Officials who authorize the extension beyond six years must record on the originator's file copy the reasons for such extension and their identity. The reasons must be specific and must explain why the classification will continue to meet the requirements set forth in subsection 2(a) above. (13 yrs 2 class extn) and EXCEPT: known (sec 4(f))

(g) Identification and Markings.

(1) Each classified document shall show on its face:

- (i) the identification of the original classification authority;
- (ii) the office of origination;
- (iii) the date of origination;
- (iv) the date or event for declassification or review;
- and (v) one of the three classification designations defined herein. No other designations, e.g., "For Official Use Only," "Limited Official Use," shall be used to identify information requiring protection in the interest of national security, except as otherwise expressly provided by statute.

(2) Each classified document shall, by marking or other means, clearly indicate which portions are classified, at what level, and which portions are not classified, in order to facilitate excerpting and other uses. Heads of agencies may, for good cause, seek a waiver of this marking requirement from the Director of the Security Information Oversight Office for certain classes of material.

(3) Classified information or material furnished to the United States by a foreign government or international organization shall either retain its original classification or be assigned a United States classification. In either case, the classification shall assure a degree of protection equivalent to that required by the government or international organization which furnished the information or material.

(4) Classified documents which contain or reveal information which the originator has determined should be subject to special dissemination and reproduction limitations shall be clearly annotated to place the recipient on notice to restrict dissemination and reproduction. In such case, the following statement shall be included in the document or on its cover sheet as a special notation separate and apart from the security classification marking:

"Reproduction of this document or portions thereof is prohibited without authorization of the originating office. Its further dissemination shall be restricted to those authorized by the addressee."

Sec. 3. Derivative Application of Markings. Persons who only reproduce, extract, summarize, or otherwise use classified information shall not be given original classification authority for the purpose of placing or directing the placement of derivative classification markings on new material if the classification is based solely on such previously classified source information. Persons who apply derivative classification markings shall respect classifications assigned by originators, and shall, to the maximum extent practicable, verify the current need for and level of classification of the information or material prior to applying such markings. They shall also carry forward to any newly created documents or material the dates or events assigned by the originator to the source material for declassification or review.

Sec. 4. Declassification. Declassification of classified information shall be given emphasis comparable to that accorded to classification. The determination to declassify information shall not be made on the basis of the level of classification assigned, but rather on the ^{the} expected perishability and loss of/sensitivity of the information with the passage of time, and with due regard for the public interest in access to official information. At the time of review, any determination not to declassify shall be based on a determination that release of the

information would be demonstrably harmful to the national security. Declassification shall be accomplished in accordance with the following:

(a) Guidelines. Within 180 days after the effective date of this Order, heads of agencies specifically named in Section 2(d) of this Order shall, in consultation with the Archivist of the United States, issue declassification guidelines which shall be applicable to 20-year old information classified under their respective jurisdictions and for which a prior automatic declassification date has not been established. These guidelines shall specifically identify those items or categories of information which, because of their probable continuing sensitivity and importance to the national security interest, cannot be automatically declassified but must be reviewed to determine whether there is a need for continued protection beyond 20 years. Information not identified in the guidelines as requiring review is and shall be automatically declassified at the end of 20 full calendar years from its date of origin. These guidelines shall be authorized for use by the Archivist of the United States and agencies having custody of the information covered therein.

(b) New Material. Information, except as provided in subsection (f), which is classified on or after the effective date of this Order, shall be declassified or reviewed for declassification in accordance with the dates

or events specified by original classification authority pursuant to Section 2(f) of this Order. Information which is not marked with a date or event for declassification or review is automatically declassified six years after its origination. Information whose classification is derived from source material/prior to the effective date of this Order shall carry forward dates or events for declassification or review shown on the source material and shall be declassified or reviewed in accordance with subsection (c).

(c) Old Material. Information, except as provided in subsection (f), which was classified before the effective date of this Order and already marked with a date or event which directs declassification in 20 years or less from the date of its origin shall be declassified in accordance with such date or event unless, upon review by officials authorized under Section 4(g) of this Order, an earlier date for declassification is determined. Such classified information not so marked is and shall be, on and after January 1, 1979, automatically declassified 20 years from the date of its origin unless identified in the guidelines issued by the heads of agencies under subsection (a) as requiring review.

(d) Systematic Review. To conserve Government resources devoted to the systematic review of 20-year old information and to achieve more effective declassification, only that information constituting the

permanently valuable records of the Government in
accordance with 44 U.S.C. 2103 shall be so reviewed. 509
Heads of agencies shall order the review of all security
classified records 20 years old or older which are
held in storage areas by the agency or in Federal Records
Centers for possible disposal. Records which are found
to be unscheduled for some definite future disposition
shall be scheduled immediately. Permanently valuable
records of the Government shall be systematically reviewed
as they become 20 years old. In the conduct of this
review the declassification guidelines issued by heads
of agencies under subsection (a) shall be applied. Only
the head of an agency designated in Section 2(d) hereof
may authorize the continued classification of information
beyond 20 years. In these cases, a declassification date
shall be determined; or, a date shall be set, not more
than ten years later, for subsequent review in accord
with these procedures established for 20 year old
information. The head of an agency or the Director
of Central Intelligence may seek a waiver of this ten
year limit. (FOR SECOND REVIEW) FROM 5100

(e) Mandatory Review. (1) All information classified
under this or prior Orders shall be subject to declassif-
ication review by the originating or responsible agency
upon request of an agency or member of the public, pro-
vided the request describes the material sufficiently
to enable the agency having custody to locate it with a
reasonable amount of effort. The head of each agency
shall designate an office to which requests for mandatory
review for declassification may be directed. After review,

the record or any reasonably segregable portion thereof which no longer requires protection under this Order shall be declassified, and released unless withholding is otherwise determined to be required under applicable statutes.

(2) Procedural instructions for processing such requests from the public shall be issued by the Security Information Oversight Office.

(3) Requests for declassification review submitted to an agency by employees thereof, shall be considered in accord with procedures which shall be established by agency heads. Denials of such requests may be referred to an agency committee for reconsideration.

(4) Material originated by a President or a President's White House staff, or material in the possession and control of the Administrator of General Services pursuant to Section 2107 or 2107 note of title 44, U.S.C., is exempted from this review if such material is less than ten years old.

Pres or private donor

(f) Foreign Originated Information. ~~Classified~~ AG
information furnished to the United States by a foreign government, international organization or an official or representative thereof, or produced by the United States

jointly with a foreign government or international organization, with the understanding that such information will be kept in confidence, shall be exempt from the declassification provisions of Section 4 of this Order. Such information shall, unless downgraded or declassified earlier, be reviewed for downgrading ^{or} and declassification 16 30 years from date of origin and shall be downgraded and declassified in accordance with guidelines developed by heads of agencies in consultation with the Archivist of the United States and, where appropriate, with the 886 foreign government or international organization concerned.

(g) Declassification Authority. The authority to downgrade ^{or} and declassify information classified under this 16 or prior Executive orders shall be exercised as follows:

(1) Classified information may be downgraded or declassified by the official who authorized the original classification, by a successor in interest or capacity, or by a supervisory official of either.

(2) Heads of agencies specifically named in Section 2(d) shall designate additional officials at the lowest practical echelons of command and supervision to exercise downgrading and declassification authority, particularly with respect to information within their areas of responsibility. These officials should also be authorized by the head of the agency to resolve conflicts or doubts regarding classification. 167

(3) The Director of the Security Information Oversight Office may downgrade or declassify information considered by the Oversight Office in the exercise of its appellate functions pursuant to Section 7 hereof, and may downgrade or declassify information in any instance wherein the Director determines that the continued classification would be in violation of this Order. These downgrading or declassification decisions shall take effect ten working days after they are made, unless during which time the head of the affected agency appeals the decision to the President through the National Security Council.

(4) In the case of classified information transferred by or pursuant to statute or Executive order in conjunction with a transfer of function and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for all purposes under this Order, including downgrading and declassification.

(5) In the case of classified information not transferred in accordance with paragraph (4) of this subsection, but originated in an agency which has since ceased to exist, each agency in possession shall be deemed to be the originating agency for all purposes under this Order. Such information may be downgraded or declassified by the agency in possession after consulting with any other agency having an interest in the subject matter.

(6) Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded and declassified by the Archivist of the United States in accordance with this Order, directives issued by Security Information Oversight Office, and pertinent regulations and declassification guidelines of the agencies.

(7) After the termination of a Presidential administration, the Archivist of the United States shall have the authority to review, downgrade and declassify information which was classified by the President, his White House staff, special committees or commissions appointed by him or others acting in his behalf when this information is not part of the records of an agency subject to Federal records statutes. This authority shall be exercised only after consultation with the agencies having primary subject matter interest.

(8) The provisions of this Order relating to the declassification of national security information shall apply to agencies which, under the terms of this Order, do not have current authority to originally classify information, but which formerly had such authority under prior Executive orders.

Sec. 5. Downgrading. Information classified under prior orders and marked for automatic downgrading is automatically downgraded accordingly. Information

classified under this or prior orders shall, after review by the originator or other official authorized to downgrade or Declassify information under this Order, be assigned a lower degree of protection against unauthorized disclosure than currently provided when such downgrading will serve a useful purpose. Downgrading action will be reflected by changing the classification to a lower level coupled with a notice of such action to holders of the information.

Sec. 6. Safeguarding.

(a) Policy Directives. The Director of the Security Information Oversight Office shall, with the approval of the National Security Council, issue directives which shall be binding on all agencies for the protection of classified information from loss or compromise. Such directives shall conform to the following policies:

(1) No person shall be given access to classified information unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of official duties.

(2) All classified information shall be appropriately and conspicuously marked to put all persons on clear notice of its classified contents.

(3) Classified information shall be used, processed, and stored only under conditions which will prevent access by unauthorized persons.

(4) Appropriate controls for classified information shall be established and maintained and such information shall be protected adequately during all transmissions.

(5) Classified information no longer needed in current working files or for reference or record purposes shall be destroyed or disposed of in accordance with the records disposal provisions contained in Chapters 21 and 33 of Title 44 of the United States Code and other applicable statutes.

(6) All classified information disseminated outside the Executive Branch shall be given appropriate protection.

(b) Secrecy Agreements. Heads of agencies may require the signing of a secrecy agreement as a precondition of access to classified information. The Security Information Office shall, in coordination with appropriate agencies, develop a uniform secrecy agreement which the heads of agencies may adopt. Secrecy agreements currently in force need not be reexecuted.

(c) Special Access.

(1) The head of an agency specifically named in Section 2(d)(1), or the Director of Central Intelligence, may impose, in conformity with the provisions of this Order, special requirements with respect to access, distribution, and protection of classified information. Special access programs may only be created

or continued by the head of an agency specifically named in Section 2(3)(1), or, for matters pertaining to intelligence sources and methods, by the Director of Central Intelligence, personally and in writing. Such special access programs shall be created or continued only on the specific showing that:

- (i) Normal safeguarding procedures are not sufficient to limit need-to-know or access;
- (ii) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and
- (iii) the special access controls balance the need to protect the information against the full spectrum of needs to use the information.

(2) All such special access programs shall automatically terminate every three years unless renewed in accordance with the procedures in this Section.

(3) Heads of agencies, or the Director of Central Intelligence as applicable, shall within 180 days after the effective date of this Order, review all existing special access programs under their jurisdiction and continue them only subject to the procedures in this section. They shall also establish and maintain for their areas of responsibility central listings of all special access programs continued or created by them. Heads of agencies, the Director of Central Intelligence, and the Director of the

Security Information Oversight Office shall have access to all such lists of special access programs; however, such right of access may not be delegated.

(d) Historical Researchers and Former Officials.

The requirement in Section 6(a)(1) that access to classified information be granted only as is necessary for the performance of one's duties shall not apply to persons outside the Executive Branch who are engaged in historical research projects or who have previously occupied policy-making positions to which they were appointed by the President; provided, however, that in each case the head of the agency:

(1) Determines in writing that access is consistent with the interests of national security;

(2) Takes reasonable action to ensure that properly classified information is not subject to unauthorized disclosure; and

(3) With respect to access granted a person by reason of his having previously occupied a policy-making position, such access shall be limited to those papers which the former official originated, reviewed, signed or received, while in public office.

(e) Controls on Reproduction and Distribution.

(1) Subject to directives issued by the Director of the Security Information Oversight Office, the heads of agencies shall ensure that:

(i) Top Secret documents are not reproduced without the consent of the originating office.

(ii) Secret documents are not reproduced except in accordance with procedures approved by an appropriate official who has been designated for that purpose by the agency having custody of the document.

(iii) No classified document is reproduced if such reproduction is prohibited by the originator and the document is so annotated.

(iv) Reproduced copies of classified documents are subject to the same accountability and controls as the original.

(v) Records are maintained by the reproducing office to show the number and distribution of reproduced copies of

Secret and Top Secret documents and those marked in accord with Section 2(g)(4) restricting reproduction and dissemination.

(2) All classified information shall be appropriately and conspicuously marked to put all persons on clear notice of its classified contents, and, if appropriate, marked to show its particular dissemination and reproduction restrictions.

Sec. 7. Implementation and Review. Overall responsibility for policy direction of the program established pursuant to this Order shall rest with the National Security Council.

(a) Overnight Office.

(1) The Administrator of General Services, subject to the direction of the President and the National Security Council, shall be responsible for the implementation and monitoring of the program established pursuant to this Order. Such responsibility shall be performed through a Security Information Oversight Office headed by a full-time Director authorized to maintain a permanent staff. The Oversight Office shall:

(i) In accordance with procedures to be established by its Director, oversee agency actions to ensure compliance with the provisions of this Order and implementing directives.

(ii) Consider and take action on complaints and suggestions from persons within and without the Government with respect to the general administration of the Order, including appeals from agency denials of requests for declassification of those classified records defined in Section 4(e)(4) which are ten or more years old.

(iii) Develop, in consultation with affected agencies, directives required for the effective implementation of this Order.

(iv) Report annually to the President through the National Security Council on Executive Branch implementation of the Executive order.

(v) Have the authority to require of each agency with original classification authority such reports, information, and other cooperation as necessary to fulfill the above responsibilities.

(2) There is also established an Interagency Security Information Advisory Committee which shall be chaired by the Director of the Oversight Office and shall be comprised of representatives of the Departments of State, Defense, Justice, and Energy, the Director of Central Intelligence, the National Security Council staff, and the National Archives and Records Service. The Interdepartmental Committee shall meet at the call of the Chairman and shall act in an advisory capacity to him in all matters related to effective implementation of this Order and implementing directives.

(b) Agencies. To promote the basic purposes of this Order, the head of each agency originating or handling classified information shall:

(1) Prior to the effective date of this Order, submit to the Security Information Oversight Office for approval a copy of the regulations it proposes to adopt pursuant to this Order and implementing directives. Subsequent changes to agency regulations shall also be forwarded to the Oversight Office for approval.

(2) Publish in the Federal Register those regulations or changes thereto which are approved by the Director of the Security Information Oversight Office and which are issued in implementation of this Order to the extent that they affect the general public.

(3) Designate a senior member of the agency staff who shall conduct an active oversight program and shall ensure effective compliance with and implementation of this Order.

(4) Designate a subordinate who shall chair an agency committee which shall have authority to act on all suggestions and complaints with respect to the agency's administration of this Order. This committee also may be authorized to act upon appeals from denials of declassification requests made pursuant to subsection 4(e).

(5) Establish a continuing program to familiarize agency personnel and others authorized access to classified information with the provisions of this Order and implementing directives. There shall also be established and maintained an active security orientation and education program for such personnel in order to impress upon each individual his or her responsibility for exercising vigilance and care in complying with the provisions of this Order.

(6) Ensure the preparation and promulgation of security classification guidance adequate to facilitate the identification and uniform classification of

information requiring protection under the provisions of this Order.

(7) Develop and promulgate declassification guidelines in accordance with Section 4(a) hereof.

(8) Take necessary action to ensure that:

(i) a demonstrable need for access to classified information is established prior to the initiation of administrative clearance procedures, and

(ii) the number of people granted access to classified information is reduced to and maintained at the minimum, consistent with operational requirements and needs.

(9) Cause a continuing review of safeguarding practices and procedures; and, eliminate those which are found to be duplicative and unnecessary.

(10) Submit to the Security Information Oversight Office such information or reports as the Director of the Security Information Oversight Office may find necessary to carry out the Oversight Office's responsibilities.

Sec. 8. Administrative Sanctions.

(a) Any officer or employee of the United States who knowingly and willfully classifies or continues the classification of information in violation of this Order or any implementing directive; or knowingly and willfully and without authorization, discloses classified information; or compromises classified information through gross negligence; or knowingly and willfully violates any other provision

of this Order or implementing directive which the head
of an agency determines to be a serious violation, shall
be subject to appropriate administrative sanctions. In
any case in which the Oversight Office finds that unneces-
sary classification or overclassification has occurred it
shall make a report to the head of the agency concerned
so that corrective steps may be taken.

(b) Sanctions may include, but are not limited to,
reprimand, suspension without pay, removal, or other
sanction in accordance with applicable law and agency
regulations.

(c) The head of each agency shall ensure that
appropriate and prompt corrective administrative action
is taken whenever a violation under paragraph (a) occurs.
Additionally, heads of agencies shall immediately inform
the Department of Justice of any case in which a violation
of the criminal law may be involved.

Sec. 9. Atomic Energy Material. Nothing in this
Order shall supersede any requirements related to "Restricted
Data" and material designated as "Formerly Restricted
Data" pursuant to the Atomic Energy Act of August 30,
1954, as amended, or the regulations of the Department
of Energy.

Sec. 10. Revocation of Prior Orders. Executive
Order No. 11652 of March 8, 1972, as amended by

Executive Orders No. 11714 of April 24, 1973 and No. 11862 of June 11, 1975, and all implementing directives issued pursuant to Executive Order No. 11652, including the Directive of May 17, 1972 (3 C.F.R. 1085(1971-75 Comp.)) are revoked.

Sec. 11. Effective Date. This Order shall become effective on March 1, 1978, except that the functions of the Security Information Oversight Office shall be effective immediately and shall be performed in the interim by the Interagency Classification Review Committee.

THE WHITE HOUSE

, 1977